UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

22801 7590 03/29/2010

LEE & HAYES, PLLC
601 W. RIVERSIDE AVENUE
SUITE 1400
SPOKANE, WA 99201

EXAMINER	
PEESO, THOMAS R	
ART UNIT	PAPER NUMBER
2432	

DATE MAILED: 03/29/2010

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/627,281	07/25/2003	Anne Kirsten Eisentraeger	MS1-1275US	4249

TITLE OF INVENTION: WEIL AND TATE PAIRING TECHNIQUES USING PARABOLAS

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1510	$300	$0	$1810	06/29/2010

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PTOL-85 (Rev. 08/07) Approved for use through 08/31/2010.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

22801 7590 03/29/2010

LEE & HAYES, PLLC
601 W. RIVERSIDE AVENUE
SUITE 1400
SPOKANE, WA 99201

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)

(Signature)

(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/627,281	07/25/2003	Anne Kirsten Eisentraeger	MS1-1275US	4249

TITLE OF INVENTION: WEIL AND TATE PAIRING TECHNIQUES USING PARABOLAS

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1510	$300	$0	$1810	06/29/2010

EXAMINER	ART UNIT	CLASS-SUBCLASS
PEESO, THOMAS R	2432	380-028000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

☐ Issue Fee

☐ Publication Fee (No small entity discount permitted)

☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

☐ A check is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/627,281	07/25/2003	Anne Kirsten Eisentraeger	MS1-1275US	4249

22801 7590 03/29/2010

LEE & HAYES, PLLC
601 W. RIVERSIDE AVENUE
SUITE 1400
SPOKANE, WA 99201

EXAMINER	
PEESO, THOMAS R	
ART UNIT	PAPER NUMBER
2432	

DATE MAILED: 03/29/2010

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 1307 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 1307 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Notice of Allowability	Application No.	Applicant(s)	
	10/627,281	EISENTRAEGER ET AL.	
	Examiner	Art Unit	
	THOMAS PEESO	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *amendment filed on 11Jun2008*.

2. ☒ The allowed claim(s) is/are *1-44*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/THOMAS PEESO/
Primary Examiner, Art Unit 2432

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Ms. Shirley Anderson on March 18, 2010.

The application has been amended as follows:

1. **(Currently Amended)** A method implemented by computer-executable instructions on a computing device for use in curve-based cryptography comprising:
determining, via the computing device, a curve for use in cryptographically processing information;
determining pairings for cryptographically processing said information using a parabola associated with said curve; [[and]]
encrypting the selected information based on the pairings[[.]]; and
outputting corresponding processed information for a curved-based cryptosystem.

2. **(Original)** The method as recited in Claim 1, wherein said at least one curve includes an elliptic curve.

3. **(Original)** The method as recited in Claim 1, wherein said pairings include Weil pairings.

4. **(Original)** The method as recited in Claim 1, wherein said pairings include Squared Weil pairings.

5. **(Original)** The method as recited in Claim 1, wherein said pairings include Tate pairings.

6. **(Original)** The method as recited in Claim 1, wherein said pairings include Squared Tate pairings.

7. **(Original)** The method as recited in Claim 1, further comprising: cryptographically processing said selected information based on said pairings.

8. **(Original)** The method as recited in Claim 7, wherein cryptographically processing said selected information based on said pairings includes decrypting said selected information and outputting corresponding decrypted information.

9. **(Original)** The method as recited in Claim 7, wherein cryptographically processing said selected information based on said pairings includes encrypting said selected information and outputting corresponding encrypted information.

10. **(Original)** The method as recited in Claim 7, wherein cryptographically processing is configured to support at least one process selected from a group of processes comprising a key-based process, an identity-based encryption process, a product identification (ID)-based process, and a short signature-based process.

11. **(Original)** The method as recited in Claim 2, wherein determining said pairings for use in cryptographically processing said selected information further includes:
determining at least a first function and a second function that are associated to certain multiples of a point on said elliptic curve;
determining said parabola that is associated with said multiples of a point, and a line associated with said parabola;
determining a third function based on said parabola and said line; and
determining said pairings based on said third function.

12. **(Original)** The method as recited in Claim 11, wherein:
said elliptic curve includes an elliptic curve E over a field K;
said first function and a second function include $f_{j,\boldsymbol{P}}$ and $f_{k,\boldsymbol{P}}$, respectively, for a point $\boldsymbol{P}$ on said elliptic curve E;
said parabola (parab) passes through points $j\boldsymbol{P}$, $j\boldsymbol{P}$, $k\boldsymbol{P}$, $-2j\boldsymbol{P}-k\boldsymbol{P}$;
said line is a vertical line through
$-2j\boldsymbol{P}-k\boldsymbol{P}=(x_4,y_4)$ having equation equal to $x-x_4$
said third function includes $f_{2j+k,\boldsymbol{P}}$ such that

$$f_{2j+k,\boldsymbol{P}}(\boldsymbol{X}) = f_{j,\boldsymbol{P}}(\boldsymbol{X}) f_{k,\boldsymbol{P}}(\boldsymbol{X}) f_{j,\boldsymbol{P}}(\boldsymbol{X}) \frac{\text{parab}(\boldsymbol{X})}{\left(x(\boldsymbol{X}) - x_4\right)}.$$

13. **(Original)** The method as recited in Claim 12, further comprising:

evaluating said parabola for at least one point selected from points $\boldsymbol{Q}$ and $-\boldsymbol{Q}$ on said elliptic curve *E*.

14. **(Original)** The method as recited in Claim 11, wherein:

said parabola (parab) has a form of

parab ($\boldsymbol{X}$) := $(x(\boldsymbol{X}) - x_1)(x(\boldsymbol{X}) + x_1 + x_3 + a_2 + \lambda_1 \lambda_2)$

$+ (\lambda_1 + \lambda_2 + a_1)(y_1 - y(\boldsymbol{X}))$; and

said third function includes $f_{2j+k,\,\boldsymbol{P}}(\boldsymbol{X})$ such that

$$f_{2j+k,\boldsymbol{P}}(\boldsymbol{X}) = f_{j,\boldsymbol{P}}(\boldsymbol{X}) f_{k,\boldsymbol{P}}(\boldsymbol{X}) f_{j,\boldsymbol{P}}(\boldsymbol{X}) \frac{\text{parab}(\boldsymbol{X})}{\left(x(\boldsymbol{X}) - x_4\right)}.$$

15. **(Original)** The method as recited in Claim 14, further comprising:

evaluating said parabola for at least one point selected from points $\boldsymbol{Q}$ and $-\boldsymbol{Q}$ on said elliptic curve *E*.

16. **(Original)** The method as recited in Claim 11, wherein:

said parabola (parab) has a form of

$$\text{parab}(\boldsymbol{X}) := (x(\boldsymbol{X}) - x_2)(x(\boldsymbol{X}) + x_2 + x_3 + a_2 + \lambda_1\lambda_2) + (\lambda_1 + \lambda_2 + a_1)(y_2 - y(\boldsymbol{X}))$$

said third function includes $f_{2j+k,\boldsymbol{P}}(\boldsymbol{X})$ such that

$$f_{2j+k,\boldsymbol{P}}(\boldsymbol{X}) = f_{j,\boldsymbol{P}}(\boldsymbol{X}) f_{k,\boldsymbol{P}}(\boldsymbol{X}) f_{j,\boldsymbol{P}}(\boldsymbol{X}) \frac{\text{parab}(\boldsymbol{X})}{(x(\boldsymbol{X}) - x_4)}.$$

17. **(Original)** The method as recited in Claim 16, further comprising:

evaluating said parabola for at least one point selected from points $\boldsymbol{Q}$ and $-\boldsymbol{Q}$ on said elliptic curve E.

18. **(Currently Amended)** A computer-readable storage medium having computer-implementable instructions for causing at least one processing unit to perform acts comprising:

determining, performed by a processing unit, at least one curve for use in cryptographically processing selected information;

calculating pairings for use in cryptographically processing said selected information by selectively using at least one parabola associated with said at least one curve; [[and]]

cryptographically processing said selected information based on said pairings[[.]]; and outputting corresponding processed information for a curved-based cryptosystem.

19. **(Currently Amended)** The computer-readable storage medium as recited in Claim 18, wherein said at least one curve includes an elliptic curve.

20. **(Currently Amended)** The computer-readable storage medium as recited in Claim 18, wherein said pairings include at least one type of pairings selected from a group of different pairings comprising Weil pairings, Squared Weil pairings, Tate pairings, and Squared Tate pairings.

21. **(Currently Amended)** The computer-readable storage medium as recited in Claim 18, wherein cryptographically processing said selected information based on said pairings includes decrypting said selected information and outputting corresponding decrypted information.

22. **(Currently Amended)** The computer-readable storage medium as recited in Claim 18, wherein cryptographically processing said selected information based on said pairings includes encrypting said selected information and outputting corresponding encrypted information.

23. **(Currently Amended)** The computer-readable storage medium as recited in Claim 21, wherein cryptographically processing is configured to support at least one process selected from a group of processes comprising a key-based process, an identity-based encryption process, a product identification (ID)-based process, and a short signature-based process.

24. **(Currently Amended)** The computer-readable storage medium as recited in Claim 19, wherein calculating said pairings further includes:

calculating at least a first function and a second function that are associated to certain multiples of a point on said elliptic curve;

calculating said parabola that is associated with said multiples of a point, and a line associated with said parabola;

calculating a third function based on said parabola and said line; and

calculating said pairings based on said third function.

25. **(Currently Amended)** The computer-readable storage medium as recited in Claim 24, wherein:

said elliptic curve includes an elliptic curve E over a field K;

said first function and a second function include $f_{j,\boldsymbol{P}}$ and $f_{k,\boldsymbol{P}}$, respectively, for a point $\boldsymbol{P}$ on said elliptic curve E;

said parabola (parab) passes through points $j\boldsymbol{P}$, $j\boldsymbol{P}$, $k\boldsymbol{P}$, $-2j\boldsymbol{P}-k\boldsymbol{P}$;

said line is a vertical line through

$-2j\boldsymbol{P}-k\boldsymbol{P}=(x_4,y_4)$ having equation equal to $x-x_4$

said third function includes $f_{2j+k,\boldsymbol{P}}$ such that

$$f_{2j+k,\boldsymbol{P}}(\boldsymbol{X})=f_{j,\boldsymbol{P}}(\boldsymbol{X})f_{k,\boldsymbol{P}}(\boldsymbol{X})f_{j,\boldsymbol{P}}(\boldsymbol{X})\frac{\text{parab}(\boldsymbol{X})}{\left(x(\boldsymbol{X})-x_4\right)}.$$

26. **(Currently Amended)** The computer-readable storage medium as recited in Claim 25, further including:

evaluating said parabola for at least one point selected from points $\boldsymbol{Q}$ and $-\boldsymbol{Q}$ on said elliptic curve E.

27. **(Currently Amended)** The computer-readable storage medium as recited in Claim 24, wherein:

said parabola (parab) has a form of

$\text{parab}(\boldsymbol{X}) := (x(\boldsymbol{X}) - x_1)(x(\boldsymbol{X}) + x_1 + x_3 + a_2 + \lambda_1\lambda_2)$

$+ (\lambda_1 + \lambda_2 + a_1)(y_1 - y(\boldsymbol{X}))$; and

said third function includes $f_{2j+k,\boldsymbol{P}}$ such that

$$f_{2j+k,\boldsymbol{P}}(\boldsymbol{X})=f_{j,\boldsymbol{P}}(\boldsymbol{X})f_{k,\boldsymbol{P}}(\boldsymbol{X})f_{j,\boldsymbol{P}}(\boldsymbol{X})\frac{\text{parab}(\boldsymbol{X})}{\left(x(\boldsymbol{X})-x_4\right)}.$$

28. **(Currently Amended)** The computer-readable storage medium as recited in Claim 27, further including:

evaluating said parabola for at least one point selected from points $\boldsymbol{Q}$ and $-\boldsymbol{Q}$ on said elliptic curve *E*.

29. **(Currently Amended)** The computer-readable storage medium as recited in Claim 24, wherein:

said parabola (parab) has a form of

$$\text{parab}(\boldsymbol{X}) := (x(\boldsymbol{X}) - x_2)(x(\boldsymbol{X}) + x_2 + x_3 + a_2 + \lambda_1 \lambda_2) + (\lambda_1 + \lambda_2 + a_1)(y_2 - y(\boldsymbol{X}))$$

said third function includes $f_{2j+k,\boldsymbol{P}}(\boldsymbol{X})$ such that

$$f_{2j+k,\boldsymbol{P}}(\boldsymbol{X}) = f_{j,\boldsymbol{P}}(\boldsymbol{X}) f_{k,\boldsymbol{P}}(\boldsymbol{X}) f_{j,\boldsymbol{P}}(\boldsymbol{X}) \frac{\text{parab}(\boldsymbol{X})}{(x(\boldsymbol{X}) - x_4)}.$$

30. **(Currently Amended)** The computer-readable storage medium as recited in Claim 29, further including:

evaluating said parabola for at least one point selected from points Q and $-Q$ on said elliptic curve E.

31. **(Currently Amended)** An apparatus comprising:

memory configurable to store information; [[and]]

logic operatively coupled to said memory and configurable to at least support cryptographic processing of selected information stored in said memory by determining at least one curve for use in cryptographically processing selected information and determining pairings for use in cryptographically processing said selected information by selectively using at least one parabola associated with said at least one curve[[.]]; and

logic operatively coupled to said memory and configurable to at least support outputting corresponding processed information for a curved-based cryptosystem.

32. **(Original)** The apparatus as recited in Claim 31, wherein said at least one curve includes an elliptic curve.

33. **(Original)** The apparatus as recited in Claim 31, wherein said logic is further configurable to perform said cryptographic processing of said selected information.

34. **(Original)** The apparatus as recited in Claim 31, wherein said pairings include at least one type of pairings selected from a group of different pairings comprising Weil pairings, Squared Weil pairings, Tate pairings, and Squared Tate pairings.

35. **(Original)** The apparatus as recited in Claim 31, wherein said cryptographic processing of said selected information includes decrypting said selected information and outputting corresponding decrypted information.

36. **(Original)** The apparatus as recited in Claim 31, wherein said cryptographic processing of said selected information includes encrypting said selected information and outputting corresponding encrypted information.

37. **(Original)** The apparatus as recited in Claim 35, wherein said cryptographic processing at least supports at least one process selected from a group of processes comprising a key-based process, an identity-based encryption process, a product identification (ID)-based process, and a short signature-based process.

38. **(Original)** The apparatus as recited in Claim 32, wherein said logic is further configured to calculate at least a first function and a second function that are associated to certain multiples of a point on said elliptic curve, calculate said parabola that is associated with said multiples of a point, and a line associated with said parabola,

calculate a third function based on said parabola and said line, and calculate said pairings based on said third function.

39. **(Original)** The apparatus as recited in Claim 38, wherein:

said elliptic curve includes an elliptic curve E over a field K;

said first function and a second function include $f_{j,\boldsymbol{P}}$ and $f_{k,\boldsymbol{P}}$, respectively, for a point $\boldsymbol{P}$ on said elliptic curve E;

said parabola (parab) passes through points $j\boldsymbol{P}$, $j\boldsymbol{P}$, $k\boldsymbol{P}$, $-2j\boldsymbol{P}-k\boldsymbol{P}$;

said line is a vertical line through

$-2j\boldsymbol{P}-k\boldsymbol{P}=(x_4,y_4)$ having equation equal to $x-x_4$

said third function includes $f_{2j+k,\,\boldsymbol{P}}$ such that

$$f_{2j+k,\boldsymbol{P}}(\boldsymbol{X}) = f_{j,\boldsymbol{P}}(\boldsymbol{X}) f_{k,\boldsymbol{P}}(\boldsymbol{X}) f_{j,\boldsymbol{P}}(\boldsymbol{X}) \frac{\mathrm{parab}(\boldsymbol{X})}{\left(x(\boldsymbol{X})-x_4\right)}.$$

40. **(Original)** The apparatus as recited in Claim 39, wherein said logic is further configured to evaluate said parabola for at least one point selected from points $\boldsymbol{Q}$ and $-\boldsymbol{Q}$ on said elliptic curve E.

41. **(Original)** The apparatus as recited in Claim 38, wherein:

said parabola (parab) has a form of

parab ($\boldsymbol{X}$) := ($x(\boldsymbol{X}) - x_1$)($x(\boldsymbol{X}) + x_1 + x_3 + a_2 + \lambda_1 \lambda_2$)

+ ($\lambda_1 + \lambda_2 + a_1$)($y_1 - y(\boldsymbol{X})$); and

said third function includes $f_{2j+k,\boldsymbol{P}}(\boldsymbol{X})$ such that

$$f_{2j+k,\boldsymbol{P}}(\boldsymbol{X}) = f_{j,\boldsymbol{P}}(\boldsymbol{X}) f_{k,\boldsymbol{P}}(\boldsymbol{X}) f_{j,\boldsymbol{P}}(\boldsymbol{X}) \frac{\text{parab}(\boldsymbol{X})}{(x(\boldsymbol{X}) - x_4)}.$$

42. **(Original)** The apparatus as recited in Claim 41, wherein said logic is further configured to evaluate said parabola for at least one point selected from points $\boldsymbol{Q}$ and $-\boldsymbol{Q}$ on said elliptic curve E.

43. **(Original)** The apparatus as recited in Claim 38, wherein:

said parabola (parab) has a form of

parab($\boldsymbol{X}$):= ($x(\boldsymbol{X}) - x_2$)($x(\boldsymbol{X}) + x_2 + x_3 + a_2 + \lambda_1 \lambda_2$)

+ ($\lambda_1 + \lambda_2 + a_1$)($y_2 - y(\boldsymbol{X})$)

said third function includes $f_{2j+k,\boldsymbol{P}}(\boldsymbol{X})$ such that

$$f_{2j+k,\boldsymbol{P}}(\boldsymbol{X}) = f_{j,\boldsymbol{P}}(\boldsymbol{X}) f_{k,\boldsymbol{P}}(\boldsymbol{X}) f_{j,\boldsymbol{P}}(\boldsymbol{X}) \frac{\text{parab}(\boldsymbol{X})}{(x(\boldsymbol{X}) - x_4)}.$$

44. **(Original)** The apparatus as recited in Claim 43, wherein said logic is further configured to evaluate said parabola for at least one point selected from points $\boldsymbol{Q}$ and $-\boldsymbol{Q}$ on said elliptic curve *E*.

2. The following is an examiner's statement of reasons for allowance: The prior art of Boneh (US Pat. No. 7,113,594) disclose cryptosystems using Weil or Tate pairings defined on an algebriac group derived form an elliptic curve (curved-based system), but do not disclose using a parabola associated with the curve to determine the pairings.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication should be directed to Gilberto Barron Jr. at telephone number (571)272-3799.

/Gilberto Barron Jr./
SPE, Art Unit 2432